Sub A6

CLAIMS

1. A method for detecting and processing attacks on a computer network, comprising:

receiving data indicating an attack may be taking place;

placing the data in a queue of data to be processed; and

processing the data in the queue.

2. The method of claim 1, wherein the step of processing includes determining the responsive action to be taken.

3. The method of claim 1, wherein the step of process includes taking action in response to the data.

4. The method of claim 1, further comprising sending an alert concerning the data to a recipient in the administrative domain in which the data was received.

5. The method of claim 4, wherein the alert comprises an e-mail message to an individual.

6. The method of claim 4, wherein the alert comprises activating a pager.

7. The method of claim 1, wherein the data is received at a first system and further comprising sharing information concerning the data with a second system in the same administrative domain as the first system.

8. The method of claim 1, further comprising sending a handoff message comprising information concerning the data to an administrative domain other than the administrative domain in which the data was received.

9. The method of claim 8, wherein the handoff message is sent directly to the other administrative domain.

10. The method of claim 8, wherein the handoff message is sent to the other administrative domain via a trusted third party.

11. The method of claim 8, wherein the handoff message is generated and sent automatically, without human intervention.

12. The method of claim 1, further comprising scanning data arriving on at least one port.

13. The method of claim 12, wherein the at least one port is a switch port and the scanning comprises copying the data passing the at least one port to a copy port associated with the switch.

14. The method of claim 13, wherein the scanning further comprises dynamically changing the port being scanned.

15. The method of claim 12, wherein the scanning comprises sending a network management protocol request.

16. The method of claim 12, wherein the scanning comprises searching the data passing the at least one port for a string.

17. The method of claim 12, wherein the scanning comprises searching the data passing the at least one port for a type of message.

18. The method of claim 12, wherein the scanning comprises searching the data passing the at least one port for an attempt to access a service known to be vulnerable to attack.

19. The method of claim 18, wherein the service is the telnet service.

20. The method of claim 1, further comprising classifying the data.

21. The method of claim 1, further comprising classifying the data by type of attack.

22. The method of claim 1, wherein the queue comprises one of a plurality of queues, wherein each queue is configured to store one or more sets of data, each set of data being associated with an event to be processed.

23. The method of claim 1, further comprising receiving a plurality of successive sets of data, each set of data comprising data concerning one event to be processed.

24. The method of claim 23, wherein the processing comprises receiving data for the next event in the queue.

25. The method of claim 24, wherein the queue comprises a plurality a queues and each successive data set is placed in a selected one of the queues.

26. The method of claim 25, wherein the plurality of queues is organized into a table of queues having at least one row and at least one column.

27. The method of claim 26, wherein the table has R rows and C columns and the selected queue is determined by calculating a row address equal to the modulus R of a first quantity associated with the data and a column address equal to the modulus C of a second quantity associated with the data.

28. The method of claim 27, wherein the first quantity is a hash value of the message containing the data.

29. The method of claim 27, wherein the second quantity is a hash value of the source address of the message containing the data.

30. The method of claim 27, wherein the processing comprises receiving and processing a next set of data from the queue, wherein the next set of data in the queue is determined by beginning at the queue from which the most recently processed set of data was taken and successively checking the next queue in order until a queue containing at least one set of data is found, and then processing the next set of data in said next queue containing at least one set of data.

31. The method of claim 23, further comprising associating an event with at least one other event to which it is related.

32. The method of claim 23, wherein a first event is associated with a second event if the first event and second event are associated with the same message.

33. The method of claim 23, wherein a first event is associated with a second event if the first event and second event are associated with the same sub-network and the event rate for that sub-network exceeds a statistically determined baseline event rate for the sub-network.

34. The method of claim 1, wherein the processing includes identifying the source of an attack.

35. The method of claim 1, wherein the processing includes tracking messages associated with an attack back to identify a point of attack at which messages associated with the attack are entering the network

36. The method of claim 35, wherein the tracking comprises:

providing a network topology map, the map including information concerning the devices that comprise the network and the ports associated with each respective device;

scanning the ports of a first device for messages associated with the attack, wherein the first device is the device from which the data associated with the attack was first received; and

identifying a first port in the first device as the port at which at least one message associated with the attack was received by the first device.

37. The method of claim 36, wherein the tracking further comprises:

determining whether the first port is an external connection to another administrative domain;

in the event that the first port is an external connection, identifying the first port as the point of attack; and

in the event that the first port is not an external connection:

identifying a second device to which the first device is connected via the first port;

scanning the ports of the second device for messages associated with the attack; and

identifying a second port in the second device as the port at which at least one message associated with the attack was received by the second device.

38. The method of claim 37, wherein successive iterations of the steps recited in claim 37 are repeated until a port is identified as the point of attack.

39. A method for detecting and processing attacks on a computer network, comprising:

receiving a plurality of sets of data each set indicating an attack may be taking place;

associating each set of data with an event;

placing each set of data in a selected one of a plurality of queues; and

processing the data associated with an event in the next queue in order after the queue from which data associated with the last event processed was taken.

40. The method of claim 39, further comprising tracking the attack back to identify a point of attack at which messages associated with the attack are entering the network.

41. A system for detecting and processing attacks on a computer network, comprising:

a computer associated with the network and configured to receive data indicating an attack may be taking place, place the data in a queue of data to be processed, and process the data in the queue; and

a database associated with the computer and configured to store data associated with suspected attacks.

42. A system for detecting and processing attacks on a computer network, comprising:

means for receiving data indicating an attack may be taking place;

means for placing the data in a queue of data to be processed; and

means for processing the data in the queue.

43. A computer program product for detecting and processing attacks on a computer network, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

receiving data indicating an attack may be taking place;

placing the data in a queue of data to be processed; and

processing the data in the queue.